БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

ФИО преподавателя: Селин А.А., канд. техн. наук

ЗАЩИТА ДАННЫХ В СООТВЕСТВИИ С КОНЦЕПЦИЕЙ ПОДСХЕМ ПОЛЬЗОВАТЕЛЕЙ

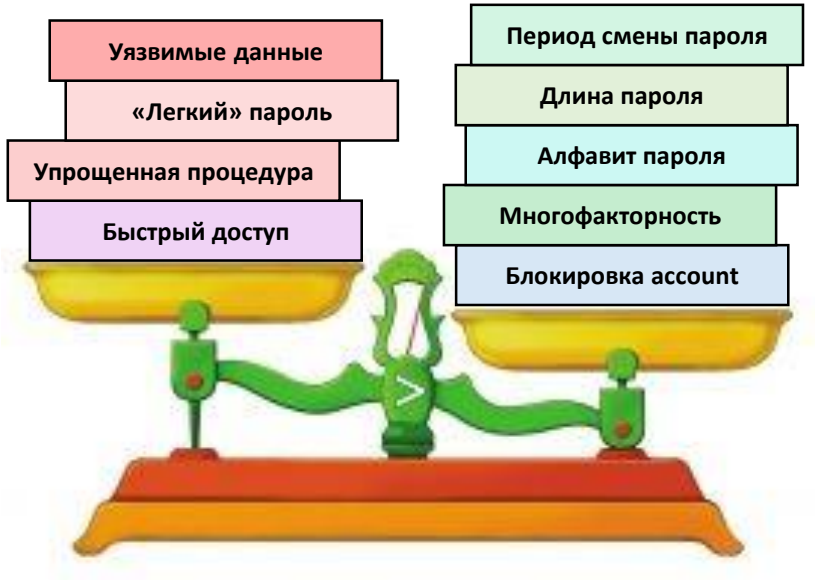
Учебные вопросы:

1. Каналы утечки в СБД
2. Механизм защиты данных на основе подсхем пользователей
3. Ведение матрицы безопасности в СБД

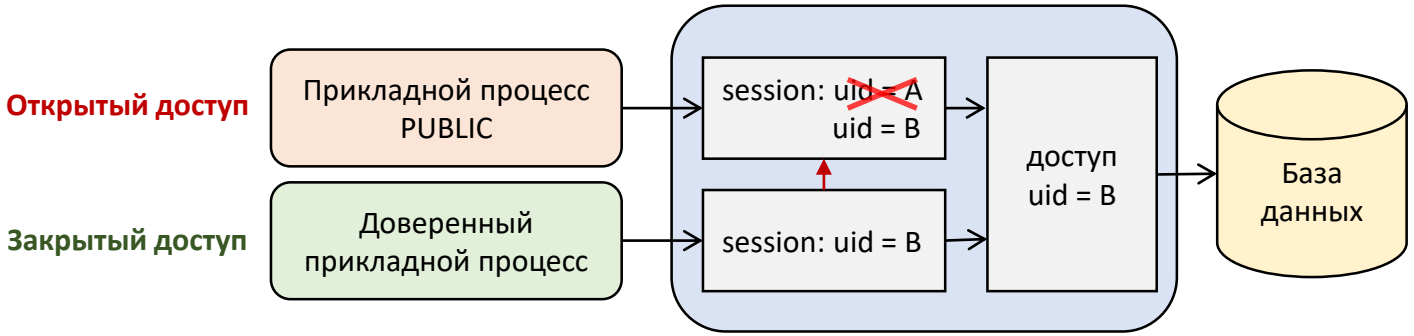
КАНАЛЫ УТЕЧКИ В СБД

Перехват паролей – завладение злоумышленником действующим паролем легитимного пользователя для последующего легального входа в систему и получения доступа к данным.

Последствия – подсистема защиты данных скомпрометирована, данные более не защищены!



Перехват полномочий – легальный процесс с низким уровнем благонадежности выдает себя за другой легальный процесс с более высоким уровнем благонадежности.

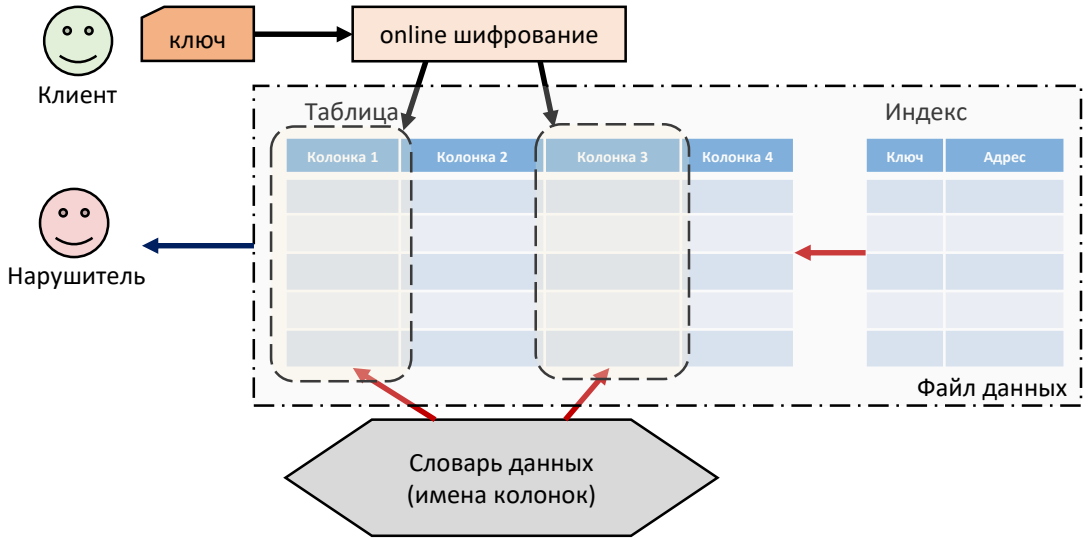


Последствия – подсистема защиты данных воспринимает прикладной процесс PUBLIC, как доверенный процесс с привилегиями обработки конфиденциальных данных,
данные более не защищены!

КАНАЛЫ УТЕЧКИ В СБД

Хищение файла данных – технически сложный процесс завладения файлом данных с последующим анализом байтовых последовательностей для восстановления конфиденциальных данных. Осуществляется агентурными или техническими методами.

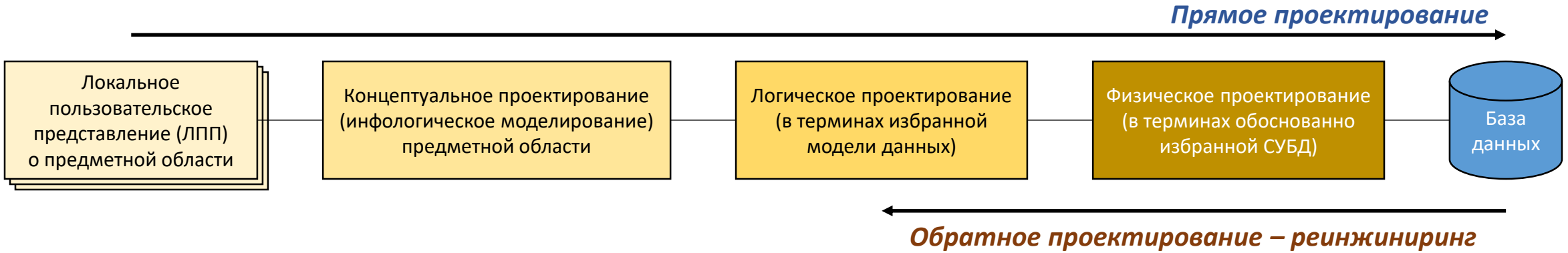
«Прозрачное» шифрование (*Transparent Database Encryption, TDE*) – механизм наложения шифра (суммирование по модулю 2) на записанные в файл данных байты данных колонок таблиц, определенных пользователем, как конфиденциальные, в режиме реального времени с использованием симметричного ключа в момент их записи и моментальное снятие шифра при чтении из файла данных.



Последствия – нарушитель имеет время и неограниченное число попыток восстановить конфиденциальные данные, выполнить реинжиниринг структуры базы данных, обнаружить ранее не известные ему сегменты базы данных (таблицы, индексы, представления, хранимые процедуры),
данные более не защищены!

КАНАЛЫ УТЕЧКИ В СБД

Вскрытие структуры базы данных (реинжиниринг) – восстановление физической и логической структуры базы данных из системного каталога. Для легитимного пользователя полезная процедура, особенно на стадии разработки и внедрения базы данных в информационную систему. Поддерживается системами автоматизированного проектирования (САПР), типа CA Erwin/ERX.



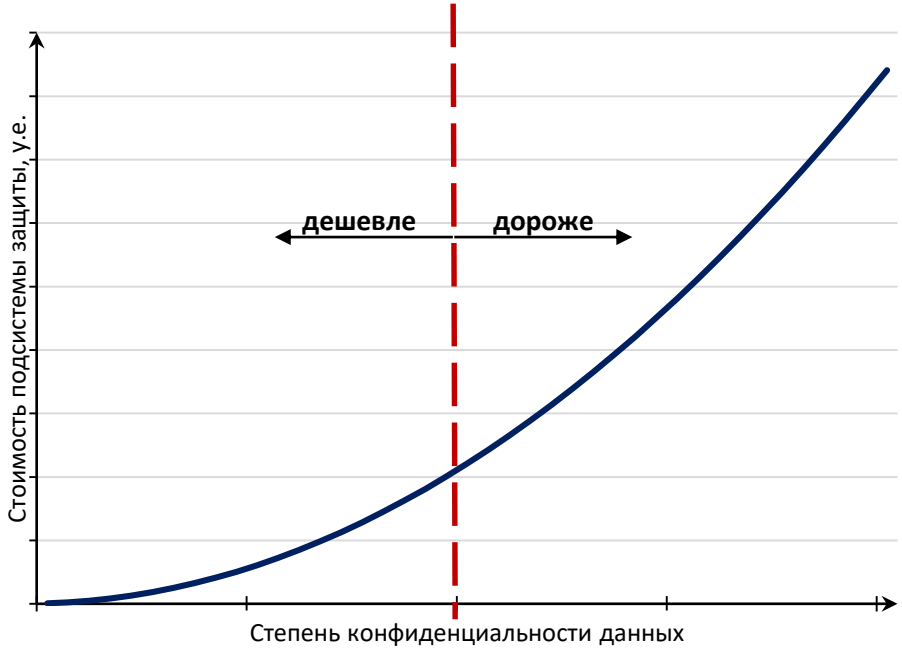
Последствия – нарушитель получает представление о колонках базы данных, предусмотренных псевдонимах, соединениях таблиц, как следствие, понимание, где хранятся конфиденциальные данные,
данные под угрозой вскрытия, нарушитель знает, что нужно искать!

Восстановление (понимание) взаимосвязи данных – на основании простых запросов к доступным данным возникает предположение, что в базе данных есть другие колонки и таблицы. «Если есть что-то недоступное, значит надо взломать базу данных и получить доступ к нему – запретный плод всегда сладок».

Последствия – нарушитель получает представление о том, что имеются колонки базы данных, где хранятся конфиденциальные данные,
возникает угроза вскрытия структуры базы данных и доступа нарушителя к конфиденциальным данным!

КАНАЛЫ УТЕЧКИ В СБД

Ошибка в определении степени конфиденциальности данных – отнесение данных с высокой степенью конфиденциальности к более низкой и, наоборот, отнесение данных с низкой степенью конфиденциальности к более высокой.



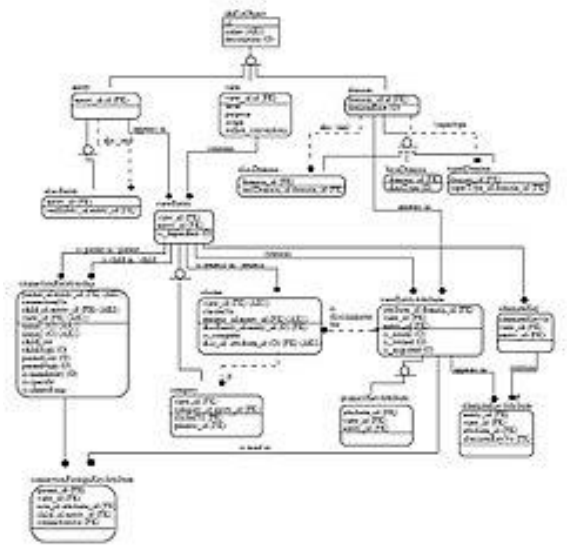
Последствия – нарушитель получает доступ к конфиденциальным данным, которые не соответствуют уровню благонадежности пользователя, учетной записью которого он воспользовался, нарушитель получает «бонус», данные более не защищены!

Ошибка в определении уровня благонадежности пользователя – предоставление пользователю полномочий, превышающих его уровень благонадежности относительно конфиденциальных данных, или ограничивающих доступ к требуемым данным.

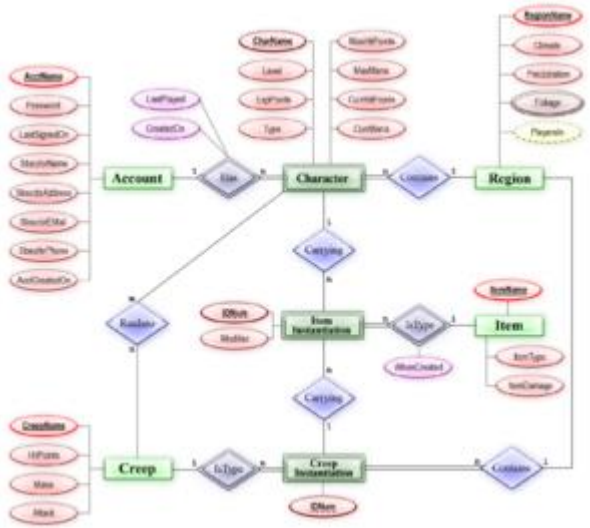
Последствия – нарушитель получает доступ к данным и функциям, которые позволяют восстановить структуру базы данных, установить наличие недоступных таблиц и сегментов базы данных, появляется возможность взлома!

МЕХАНИЗМ ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ПОДСХЕМ ПОЛЬЗОВАТЕЛЕЙ

Схема базы данных (англ. *Database schema*) — её структура, описанная на формальном языке, поддерживаемом СУБД.



=



=

```
CREATE TABLE tabl1 (
        atrib1 INT NOT NULL,
        atrib2 VARCHAR2(200)
        atrib3 DATE );
CREATE TABLE tabl2 (
        atrib1 INT NOT NULL,
        atrib4 INT NOT NULL,
        atrib5 TIMESTAMP,
        atrib6 VARCHAR2(150) );
ALTER TABLE tabl1 ADD PRIMARY KEY (atrib1);
…
```

Подсхема (схема, schema) пользователя – это объект базы данных, логически объединяющий в изолированную именованную группу некоторую заданную пользователем совокупность объектов базы данных (таблиц, индексов, представлений, хранимых процедур, функций, последовательностей и т.п.).

Подсхема пользователя обладает свойством инкапсулированности.

В ORACLE и MS SQL Server жестко закреплена за пользователем-владельцем, в PostgreSQL – может быть независимой от пользователя и обеспечивать доступ к своим объектам одновременно нескольким пользователям.

МЕХАНИЗМ ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ПОДСХЕМ ПОЛЬЗОВАТЕЛЕЙ

Управление подсхемой (схемой) пользователя:

создание схемы
```
CREATE SCHEMA <имя_схемы>;
```

создание схемы с заданным именем и владельцем
```
CREATE SCHEMA <имя_схемы> AUTHORIZATION <имя_учетной_записи>;
```

создание схемы с именем, совпадающим с именем владельца
```
CREATE SCHEMA AUTHORIZATION <имя_учетной_записи>;
```

обращение к таблице из схемы
```
<имя_схемы>.<имя_таблицы>
```

перемещение таблицы в существующую схему
```
ALTER TABLE <имя_таблицы> SET SCHEMA <имя_схемы>;
```

переименование схемы
```
ALTER SCHEMA <имя_схемы> RENAME TO <новое_имя_схемы>;
```

переопределение владельца схемы
```
ALTER SCHEMA <имя_схемы> OWNER TO <имя_учетной_записи>;
                                  | CURRENT USER | SESSION USER
```

удаление схемы
```
DROP SCHEMA <имя_схемы> [CASCADE];
```

проверка последовательности просмотра схем
```
SHOW search_path;
```

```
SQL> SHOW search_path;

search_path
-----------------
"&user", public
```

просмотр начинается со схемы пользователя

КАНАЛ УТЕЧКИ! Схема public доступна всем!

МЕХАНИЗМ ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ПОДСХЕМ ПОЛЬЗОВАТЕЛЕЙ

Подсхема (схема) public – это создаваемая автоматически общедоступная схема, в которую помещаются все вновь создаваемые объекты базы данных, если для них не указано имя схемы.

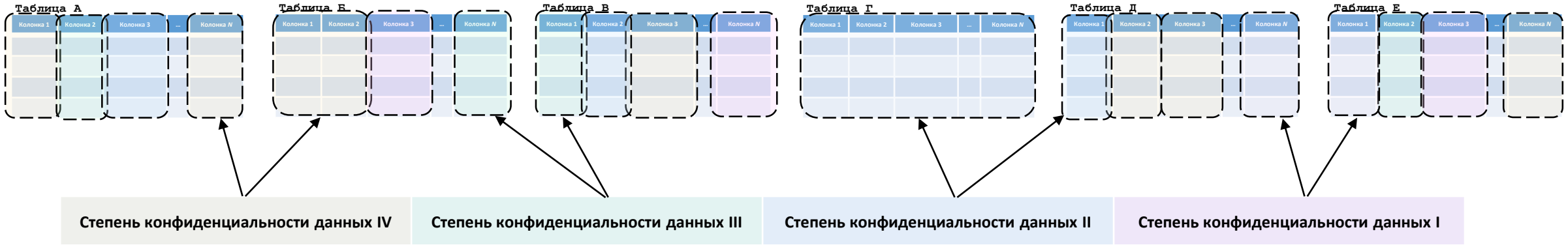
```
CREATE TABLE <имя_таблицы> (…);   ≠   CREATE TABLE <имя_схемы>.<имя_таблицы> (…);
```

будет помещена в схему public

будет помещена в схему **<имя_схемы>**

Концепция защиты базы данных на основании подсхем (схем) пользователей

1. Распределить все объекты базы данных по степеням конфиденциальности – присвоить каждому объекту метку конфиденциальности.



МЕХАНИЗМ ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ПОДСХЕМ ПОЛЬЗОВАТЕЛЕЙ

2. Распределить все субъекты обработки данных по уровням благонадежности – присвоить каждой учетной записи метку благонадежности.

Ограничить обычных пользователей личными схемами.

```
REVOKE ON SCHEMA public FROM PUBLIC;
```

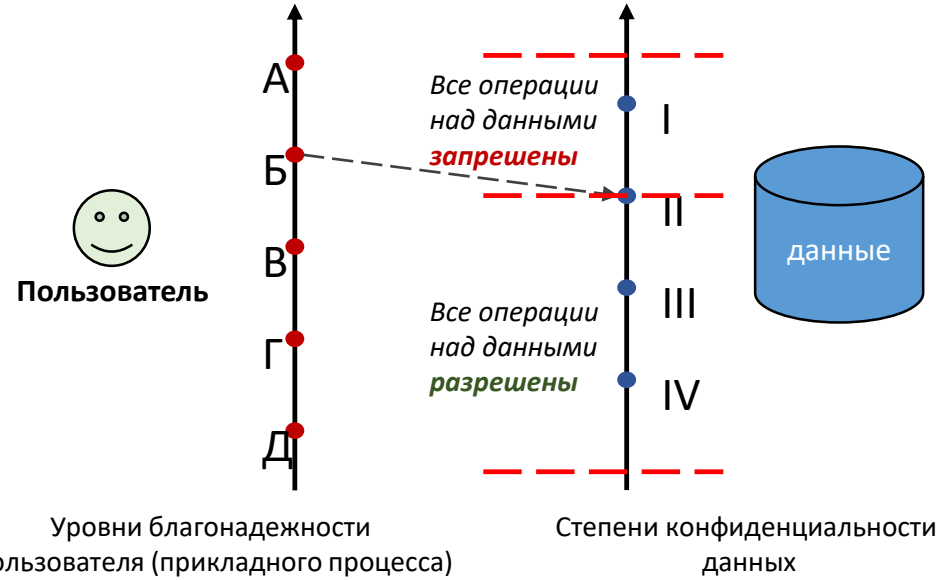
Удалить схему public из пути поиска по умолчанию для каждого пользователя.

```
ALTER ROLE <имя_учетной_записи> SET search_path = "$user";
```

Пометить каждую учетную запись меткой уровня благонадежности.

3. Определить правило соответствия степеней конфиденциальности данных уровням благонадежности пользователей.

Основное свойство (main property) механизма защиты – пользователь имеет полный доступ к данным, когда степень их конфиденциальности соответствует или ниже его уровня благонадежности и не имеет никакого доступа к данным со степенью конфиденциальности, превышающей его уровень благонадежности.



4. В соответствие с основным свойством концепции сформировать правила назначения полномочий учетным записям пользователей.

```
GRANT SELECT ON <имя_схемы>.<имя_таблицы>,
      INSERT ON <имя_схемы>.<имя_таблицы>,
      UPDATE ON <имя_схемы>.<имя_таблицы>,
      DELETE ON <имя_схемы>.<имя_таблицы>
 TO <имя_учетной_записи>;
```

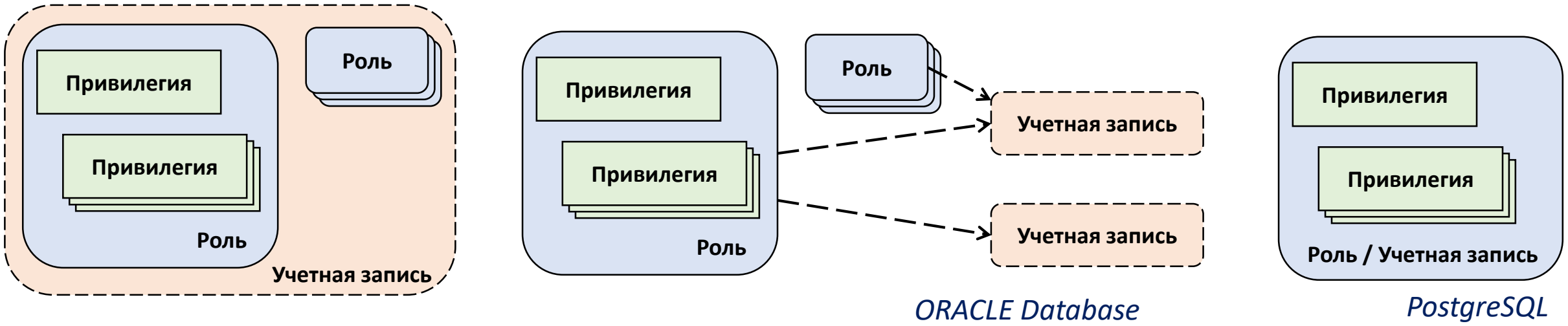
5. Разработать матрицу безопасности. Присвоить учетным записям пользователей полномочия в соответствие с матрицей безопасности.

ВЕДЕНИЕ МАТРИЦЫ БЕЗОПАСНОСТИ В СБД

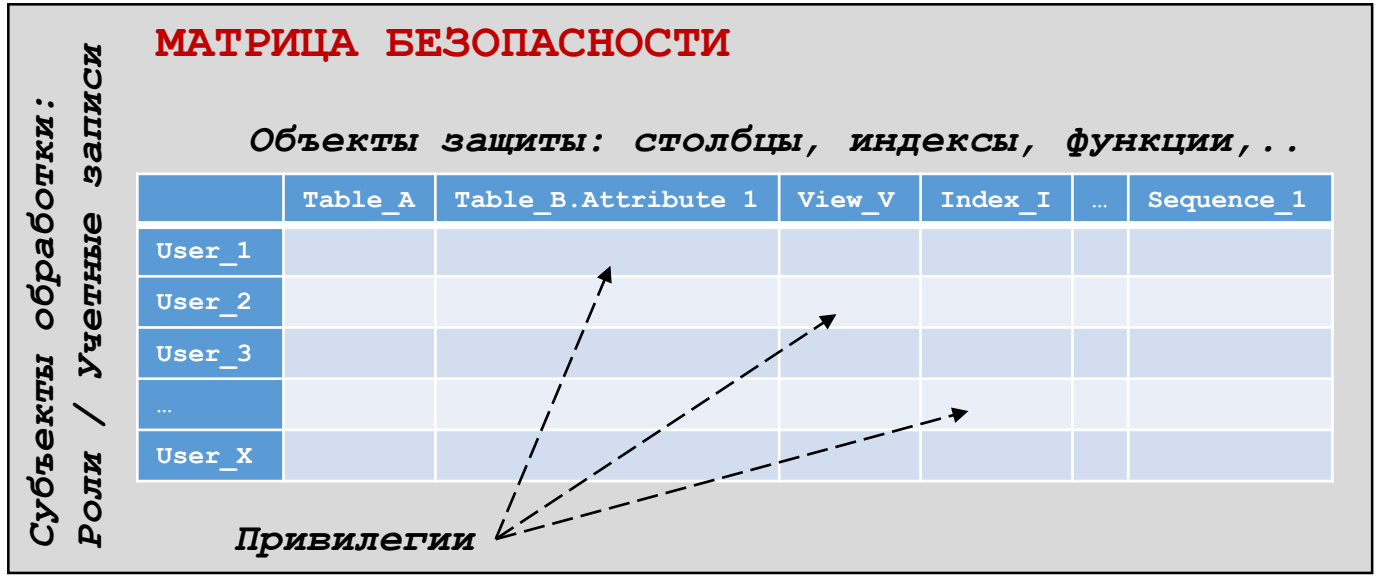
Привилегия (англ. *privilege*) – право пользователя (пользовательского процесса) на «прикосновение» к данным с указанием, что он может с ними сделать (вставить, удалить, модифицировать, выбрать,..) или выполнение какой-либо работы в базе данных, в том числе подключение к ней.

Роль (англ. *role*) – комплект **привилегий** для типовой работы пользователя в соответствие с его функциональными обязанностями в учреждении (например, кассир билетной кассы, бухгалтер по проводке оплаты труда, оператор склада, специалист по снабжению, руководитель основного подразделения, менеджер торгового зала,…). Комплект привилегий зависит от бизнес-модели (совокупности бизнес-процессов), реализованной в учреждении.

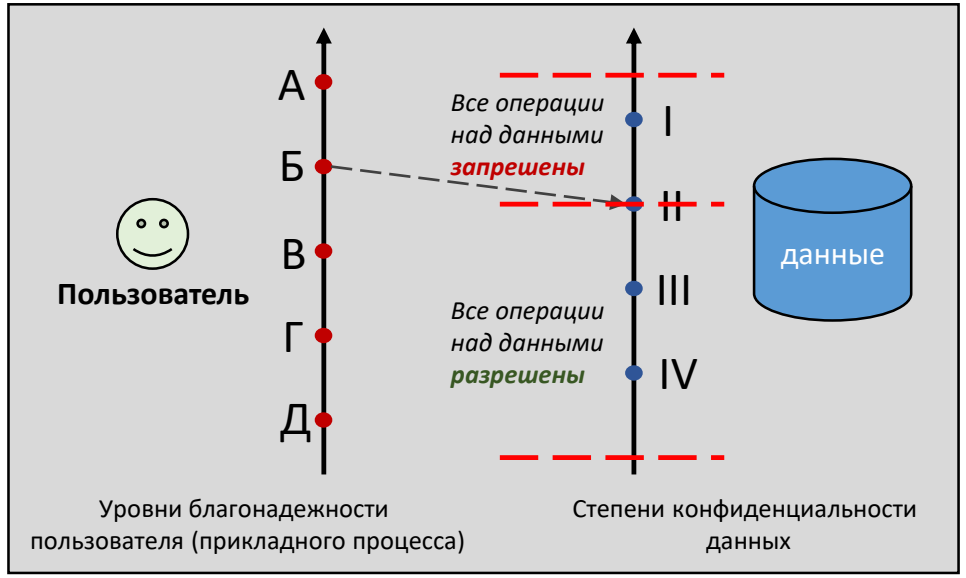
Учётная запись (англ. *account*) – хранимая в системе баз данных совокупность атрибутов пользователя, необходимая для его опознавания (аутентификации) и предоставления доступа к данным, пользовательским объектам, системным объектам, функциям системы и настройкам.



ВЕДЕНИЕ МАТРИЦЫ БЕЗОПАСНОСТИ В СБД



+



= Механизм защиты базы данных

Матрица безопасности в явном виде не доступна НИКОМУ, включая и администратора безопасности!

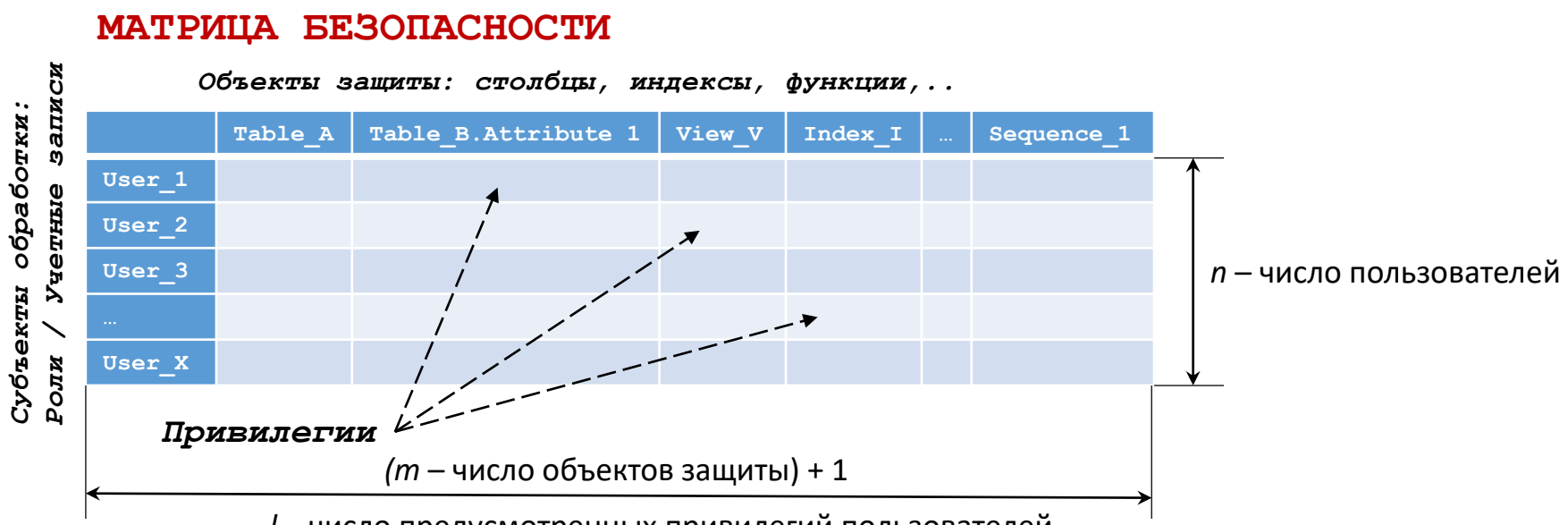
Матрица безопасности физически представляет собой совокупность спецификаций, хранящихся в словаре данных системы баз данных.

Назначая полномочия ролям и учетным записям пользователей администратор безопасности автоматически вставляет, удаляет или обновляет записи в матрице безопасности.

Чтение записей из матрицы безопасности выполняет подсистема защиты базы данных в момент обращения пользователя на подключение.

Джентльменский набор полномочий (ролей в терминах СБД ORACLE Database): **CONNECT (LOGIN), RESOURCE**

ВЕДЕНИЕ МАТРИЦЫ БЕЗОПАСНОСТИ В СБД



кодирование названия привилегии t символами

обеспечение целостности матрицы – первичный ключ (объем до 10 байт)

$$V_{\text{мб}} = n \times (l \times t \times (m+1) + V_{PK})$$

Меры повышения защищенности системы баз данных:

1. Оценка объема матрицы безопасности.
2. Аудит матрицы безопасности.
3. Модифицированные матрицы безопасности – уточнение привилегий пользователей.

Литература:

1. **Смирнов, С. Н.** Безопасность систем баз данных [Текст]: учеб. пособие для вузов по специальностям в области информационной безопасности. – М.: Гелиос АРВ , 2007. – 350 с.

2. **Федин, Ф. О.** Информационная безопасность баз данных. Ч. 1 [Электронный ресурс]: учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — М.: РТУ МИРЭА, 2020. — Электрон. опт. диск (ISO)

3. **Терьо, М.** Oracle. Руководство по безопасности [Текст] / М. Терьо, А. Ньюмен; Пер. с англ.. — М.: Лори, 2004. — 560 с.: ил.

4. **Советов, Б. Я.** Базы данных: теория и практика : Учебник для вузов / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — М.: Высш. шк., 2005. — 464 с.: ил.

5. **Саймон, А.** Безопасность баз данных. // СУБД № 1, 1997 г. – с. 78 – 95.

6. **Кузнецов, С. Д.** Основы баз данных: курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. ин-форм. технологий / С. Д. Кузнецов. – Москва: Интернет-ун-т ин-форм. технологий, 2005. – 488 с.

7. **Смирнов, С. Н., Задворьев, И. С.** Работаем с ORACLE.: Учебное пособие/2-е изд., испр. и доп. – М: Гелиос АРВ, 2002 г. – 496 с.

8. **Кульба, В.В.** и др. Теоретические основы проектирования оптимальных структур распределенных баз данных. – М: СИНТЕГ, 1999 г. – 660 с.

9. Материалы сервера ORACLE/RE. www.oracle.ru/press/magazine/main.html

10. Материалы информационного ресурса WIKIPEDIA. https://ru.wikipedia.org/wiki/Разграничение_доступа_на_основе_атрибутов; https://ru.wikipedia.org/wiki/Аутентификация; https://ru.wikipedia.org/wiki/Многофакторная_аутентификация; https://ru.wikipedia.org/wiki/Сложность_пароля.